CANDID COMMUTATORS

Ludvig Sylows' Theorems On The Groups of Substitutions

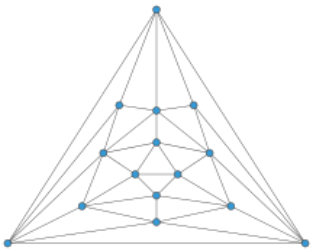
Author: Owino Stephen

Publisher: ©2021 This book was typeset using LaTeX Program

Date: November. 26, 2021

Version: 1.0

Bio: https://github.com/StevenOwino



Learning is an ornament in prosperity, refuge in diversity, and a provision in old age.

Contents

0.1 Preface 1

1 Fermats' Conjecture **2**

1.1 Introduction 2

1.2 Commutators 3

1.3 Keywords 4

2 Deconstruction Of The Proof **6**

2.1 Computing Cohomology Groups 6

2.2 Group Transformation 6

2.3 Ring Properties 7

2.4 Andrew Wiles' Main Conjecture 7

2.5 Quadrature Units Of Rotation 8

2.6 General Concerns Regarding Problems Of The Proof 8

2.7 Conclusion 8

3 Theorems On The Groups Of Substitutions **10**

3.1 Theorems On The Groups Of Substitutions: 584 10

3.2 Theorems On The Groups Of Substitutions: 585 10

3.3 Theorems On The Groups Of Substitutions: 586 11

3.4 Theorems On The Groups Of Substitutions: 587 12

3.5 Theorems On The Groups Of Substitutions: 588 13

3.6 Theorems On The Groups Of Substitutions: 589 14

3.7 Theorems On The Groups Of Substitutions: 590 14

3.8 Theorems On The Groups Of Substitutions: 591 15

3.9 Theorems On The Groups Of Substitutions: 592 16

3.10 Theorems On The Groups Of Substitutions: 593 17

3.11 Theorems On The Groups Of Substitutions: 594 18

A Mathematical Tools **20**

A.1 Probability Measure 20

0.1 Preface

The cover photo of the book(a dihedral group), is a Geometric representation in the complex plane. The complex conjugate is found by reflecting across the real axis.

Note *The technique applied for the presentation in the proceeding chapters is well known, and is based on adjoining of roots of simple irreducible equations with the properties of radical solubility.*

SPECIAL SYMBOLS:

1. ϑ : Variable theta
2. φ : Variable phi
3. γ : gamma
4. $\dim$: Dimensions of linear systems
5. $\rightarrow$: Maps to
6. $|$: Divides
7. $|x|$: Absolute Value of x
8. $\mathrm{tr}\ y$: Trace y
9. $\overline{T}$: Closure
10. $\leftrightarrow$: If and only If (iff)
11. $||G||$: Norm of partition G
12. $\equiv$: Modulus(logical equivalence)

```
The content of the book is based on spaced structuring, and iterative deepening.
```

I would like to thank Peter, Irene, Josephine, Becky and the Overleaf team for making the impossible happen.

Chapter 1 Fermats' Conjecture

Let us examine if the proof of FLT is complete. This will be leverage for translating Ludvig Sylows' paper "On The Theories of Group Substitutions". For any questions, suggestion or comment, feel free to contact me on GitHub issues or email me at stowino21@gmail.com.

The following are prerequisites to appreciate the content of the presentation:

- Courage: A mature level of technical competence. We shall study in depth, but without complete rigour the concepts of modular elliptic curves and its association with Fermats' Last Theorem. A claim that it has the property of a radical solvable equation. This account does not provide a derivation of measurement and frequency, but the pragmatic attitude taken is that it clarifies its Mathematical and Physical origin.
- Grammar: Polynomials, Vector(Gauge)Fields, Groups(Semi-simple conjugacy class), and Rings.
  In Number Theory,

$$x^n + y^n = z^n \text{ has no integer solutions where } n > 2 \text{ and } x, y, z \neq 0 \tag{1.1}$$

We begin with Lefschetz' fixed-point Theorem which generalizes the use of an identity matrix so that each trace term is the dimension of the appropriate cohomology group. That is, an Identity Map = Euler characteristic(In other words, its an alternating sum of numbers of the space.)
Now, every continuous map from the n-dimensional closed space(unit disk) must have at least one fixed point or pole. Let

$$f : D_n \to D_n \tag{1.2}$$

where D_n is compact and triangulable; All of its homology groups except $H_\circ$ are zero, and every continuous map induces an identity map whose trace $= 1$. So this implies that the identity matrix is non-zero for any continuous map. This is based on the construction of identical field equations arising from Lagrangian densities, specifically those of $O(n)$ gauge theory, whee it is transparent that the Lagrangian is invariant under a transformation.

1.1 Introduction

1. **MOTIVATION**: A less condescending, and candid review of Andrew Weils' proof of Fermats' Last Theorem, and to avoid guessing things which are obviously false. ;
2. **OBJECTIVE**: We shall have a considerable degree of understanding on the techniques of congruent relations between modular forms. This will be achieved by finding the relevant properties of fitting ideals, specifically on regular sequences(Also known as an isomorphism of integer ring module as an R-module) ;
3. **CLAIM**: By construction of the the maximal ideal(i.e, a $\dim \leq 1$, referencing Riemann-Roch Theorem)....For a finite ring type over the ring of integers, there exists an N such that for each $\imath$, $x_\imath^N$ can be written in the ring type as a polynomial of total degree less than N. That is to say, its a factorization of a finite simple group. This general formulation is necessarily borrowed from the very circular discussions of observables with continuous spectrum, such as the position operator x on

$$H = L^2(\mathbb{R}) \tag{1.3}$$

for a particle moving in one dimension, relies on the Spectral Theorem for self-adjoint operators on Hilbert Space.;

1.2 Commutators

The existence of complete intersections on a curve, with Abelian varieties over the ring integer modules is well known. For our case, a non-trivial decomposition i.e, ring modules with no intersection of the co-primes, relates to a sequence of maps in which the adjoints are an isomorphic function composition satisfying the required relation of a complex conjugate, and congruency. In other words, the existence of two different modular forms gives the same representation, and thus describes the size of congruent numbers which are related to both the subspace, the modular form, and of the the elliptic curve. This kind of mapping, as quotients of group rings arising from n-dimensional representations, produces congruent primes. Robert Langlands clearly demonstrates in his lectures by pointing out the techniques applied: Take the Geometric Anatomy of Physics, interpret as Spectral Theory(i.e, construct the structure of operators in a variety of Mathematical spaces) in Hilbert Space, then we'll now be able to define the orthogonality of an inner product in a given Vector Space; This is commonly referred to as a commutative family of integral operators.

1.2.1 Consistency Of The Proof

The proof of Fermats' Conjecture is treated and accepted as fairly consistent due a corresponding proof of a VANISHING DIMENSION i.e, a unitary matrix, which is restricted to the cyclic(direct co-prime product) Sylow p-subgroup, where the order of the subgroup has a cardinality of power p in an unramified extension of cyclotomic fields by the adjointness of a complex root of unity to $\mathbb{Q}$. In addition, a rotation in a quasi-dihedral group proves that there exists an identity map invariant in the class field. This argument is lifted from the assumption in Gauge Theory stating that the mass of a photon vanishing in an electromagnetic field is NOT isotopic invariant i.e, the symmetry group is non-commutative! Now for a given subtle case: The diagonal matrices commuting implies that the order of a Sylow p-groups of $GL_2(F_q)$ is P^{2n}: where p and q are primes greater than or equal to 3; And P is also congruent to $1(mod\ q)$. The order of $\{GL_2(F_q)\}$ is

$$(q^2-1)(q^2-q) = q\ (q+1)(q-1)^2 \tag{1.4}$$

Since

$$q = p^n(m+1) \tag{1.5}$$

the order of

$$GL_2(F_q) = P^{2n}m \tag{1.6}$$

The theorem is thus proved. You must at this point be able to clearly see the substitution in the exponent! Therefore, exploiting the control of conjugacy in derived subgroups, defines the case above, or rather, the sort for elements used in classifying the finite simple groups, and of course, whose Sylow p-group is a quasi-dihedral group. The corresponding localized pre-image in the abstract Hecke ring, in the case above of $GL_2(F_q)$ is generated as a polynomial ring by all the standard Hecke operators in the Theory of Modular Forms. That is to say, Its an Algebra of bi-invariant measures under convolution. For example, in Electrical Engineering, the convolution of one function(the input signal) with a second function(the impulse response) gives the output of a linear time-invariant system, also known as LTI. Thus, at any given moment, the output is an accumulated effect of all the prior values of the input function, with the most recent values typically having the most influence, i.e, the output function is expressed as a multiplicative factor.

Remark A Convolution function is an operation on two functions $f\ and\ g$ that produces a third function $(f * g)$ which expresses how the shape of one is modified by the other. For our purpose, this can be defined as the

integral of the product of two functions after one is reversed and shifted. The integral is then evaluated for all values of shift, producing the convolution function. This is by far the only approach to prove that the existence of the class fields is CONSISTENT.

1.2.2 Definitions

We now need to quickly familiarize with a few very important definitions to assist with comprehending the subsequent sections.

The entire material is based on the premise of a cycle into a cycle extended to LC Spaces:

Definition 1.1

LC Spaces -- An absolute neighborhood retract
Deformation(Permutation) -- Transformation of a chain and its boundary extended to absolute neighborhood retracts on R, into a homologous cycle
Cohomology group -- A Representational Space
Ring of Integer Module -- A complete valuation ring
Probability Measure -- The restriction of the total state on A to the "classical" sub-algebra D
Infinite sequence of measurement -- Proof that any ensuing frequencies automatically satisfy the Born Rule

♣

Definition 1.2

R : The universal local flat deformation ring of $\rho_\circ$. Also Known as the initial local representation for ring algebras.
R^{fl} : The tensor product corresponding ring of the Galois algebras

♣

The strategy of the proof that follows in the next section is then to construct a bi-linear pairing of multiplicative reduction of finite rank, which can be mapped to the ring of integers such that both the maps form a sequence of isomorphisms. This is the method applied and related to Ludvig Sylows' "Theorems On The Groups Of Substitutions", which was the motivation for the English translation of "Theoremes Sur Le Groupes De Substitutions". Unfortunately still, there will be NO royal roads in this study.

1.2.3 Lesson

You are completely on your own tackling these daunting subjects, and their associated problems. Find the courage to continue forth.
Your confidence, or skepticism will depend on your temperament, and largely to your own interest.

1.3 Keywords

For some reasons, we will need to list the essential vocabulary you will come across in your quest of understanding group order(regular reduction of a simple group).
Remark We all do this by other great mens' writing, so that we can come easily by what they have labored hard for us:

Piree Fermat, Solomon Leftschetz, Leonard Euler, Joseph Louis Lagrange, Georg Riemann, Gustav Roch, Neils Abel, Robert Langlands, David Hilbert, LUDVIG SYLOW, Ernst Kummer, Robert Mills, Yang Chen-Ning, Carl Gauss, Everiste Galois, Erich Hecke, Sophus Lie, Jean -Marc Fontaine, Ferdinand Frobenius, Jean-Pierre Serre, John Tate, Carl Jacobi, Joseph Liouville, Karl Weistrass,...

Modular forms, Conjugacy, Trace, Maximal Ideal(Identity Matrix), Homology, Congruent, Ring Type, Factorization, Mapping, Prime Number, Simple Group, Spectral Theory, Vector Space, Commutative, Sylow p-group, Co-prime, Cyclotomic Field, Rational Numbers, Quasi-Dihedral Group, Gauge Theory, Orthogonal group O(n), Yang-Mills Theory, Gauge Field, Abelian(Non-Abelian Group), Modulus, Lie Group(Algebra), Galois Extension(Algebraic Field Extension), Hecke Algebra(Ring), Locally Compact Group, Convolution(Function), Invariance, LTI-System, Theory Of Fontaine, Groups Of Bloch-Kato, Tate Local Duality, Atiya-Bott Metric Space, Gorenstein Rings, Riemann Hypothesis,...

Chapter 2 Deconstruction Of The Proof

Consider deformations of Galois representations i.e, construct its contra-gradients. Compute R^{fl}, which is the ring for Galois group of Algebras to find a sequence of p-divisible groups. These are the ring of integers generated by Fourier coefficients to obtain a restriction map of localization. This is a process of commuting continuous Galois Action W_λ on K-Vector spaces. Consider Selmer deformation: A map of ring algebra modules tensored to yield a continuous homomorphism. This defines the local cohomology group. We can now relate the above with the Theory of Fontaine and the groups of Bloch-Kato. Therefore, the dual of a manifold, which is a family of elliptic curves with a Cartier Twist, is considered to be a semi-stable reduction. That is to say, its a matrix transformation. So, under the cusp, known as the closed subspace, or product pairing with respect to quotients and subgroups, the orthogonal complement of the unramified homomorphisms is the image of the units.

2.1 Computing Cohomology Groups

Consider the Theorems of Poitou and Tate to order the sequences, and to ESTIMATE the cohomology group. It is concluded that

$$R \simeq R^{fl} \leftrightarrow r = 2 \tag{2.1}$$

where r is the dimension of the Bloch-Kato cohomology group. Below is some result of an exercise on the subgroup $GL_2(K)$:

```
First assume that the determinant of the local representation is ODD. It then follows that
    the order of the derived group must have eigenvalues of -1, since it is the kernel of
    the determinant.
The extended scalars, which are of course Linear Algebraic, commute with formation of duals
    and cohomology groups. This a precise proof that satisfies the required rule of
    commutator relation(self-adjointness) for finite-dimensional vector space.
```

We can now assert that: For a local projection(which is a mapping of a smooth variety over an Algebraically closed field) of a Galois tensored space for any +ve integer n, and any irreducible Galois stable subspace, there EXISTS a $\{\sigma\}$ in the Galois subspace, where $\{\sigma\}$ is the sort for elliptical differential operator on the supposed vector bundle. This is a construction technique by Atiya-Bott metric space.
Remark Refer to the **Theorem 3.4(IV)** of Ludvig Sylows' **"Theorems On The Groups Of Substitutions"** for the next section.

2.2 Group Transformation

For an Abelian Group, it is possible to construct a sum of three distinct quadratic characters for a quadratic field associated to $\{\delta\}$, where $\{\delta\}$ is an an inverse factor, and its derivative is clearly not square-integrable.[1] Therefore, LC, the extension to an absolute neighborhood retract, is then implemented using a complex-valued function. Again here, $\{\sigma\}$, which is now a TRACE, with the property of an element of both the Galois

[1]Refer to my Youtube video "Principle Of The Reciprocal".

and cohomolgy groups, has a categorical trace of 0. That is to say, a matrix capturing alternating sums of ranks(cells). This implies too that the eigenvalue is equal to 1.

Precisely, $\{\sigma^2 = 1\}$ since $\{\rho_\circ \mid L\}$ is absolutely irreducible where

$$L = Q\sqrt{(-1)^{(p-1)/2p}}. \tag{2.2}$$

This is indeed a finite singular complex transform. [2] If a transformation T is a continuous single valued transformation of LC- Space R into itself, without fixed points, the invariant $\{\sigma T = 0\}$. Therefore, a sufficient condition of fixed points is that $\{\sigma \neq 0\}$. So now,

$$\sigma\overline{T} = \sum(-1)^p \text{ tr } y^p = \sigma T \tag{2.3}$$

where $\{\sigma\}$ is a function of the homology class of the transformation, and $\{y^p\}$ is a base for the p-group.

2.3 Ring Properties

Global functionality can then be obtained using a stable trace formula on a given Frobenius endomorphic vector space. Thus, a SHEAF(computable Euler stack), also known as Arithmetic Frobenius, of regular differentials has the property of containing a p^{th} ROOT of UNITY. That is, sequences of TANGENT SPACES. It thus follows that the CONGRUENCES between the rings, in this case, is an action of the Hecke Operators on the kernel of the restricted maps. This is possible since Euler Products are defined by means of the Hecke Operator $\{\lambda_f\}$. Indeed, conjugation by matrices induces isomorphism. This is to say, a change of group of cohomology to the cohomology of the associated curves are NILPOTENT.[3] In other words, the intersection of the subgroups is equal to 1. It is useful to know that an abstract Hecke Ring, which is abstract complex, is generated by a polynomial ring using standard Hecke Operators. Meaning... the cohomology groups have genus 0, and are TORSION FREE (The cohomology groups are topologically invariant in a Riemann surface). Let us now proceed to a brief discussion on product representation of Galois conjugate classes of eigen forms.

2.4 Andrew Wiles' Main Conjecture

A proof is constructed showing that a minimal Hecke Ring is a complete intersection. Furthermore, a map is also an isomorphism for all deformations associated with local representations, as long as the local representation is modular i.e, a dihedral extension, absolutely irreducible, and restricted. Computations of Selmer Group is then possible using a topological generator and is achieved by integrating the projective limits of the product of local principal units, and factoring to define the continuous isomorphism. The result is that we get a PRIME from the ring of integers such that the associated local representation satisfies congruency. That is to say, we obtain a linear map on homology coming from complex conjugation on the given curve. Take

$$R_d = T_d \tag{2.4}$$

This means that the universal local deformation of the ring is equal to the deformation of certain ring type, which is of course a complete intersection. Thus, a local representation is associated to a modular form of weight $\{K \geq 2\}$. Considering some results on elliptic curves:

```
It is known that the image of certain irreducible curves of non-trivial degree can be
    classified satisfying rational points corresponding to modular elliptic curves.
```

[2] Refer to the proof of Theorem II by Lefschetz on his paper **"On The Fixed Point Formula"**

[3] "Refer to Ben Greens' Lectures on **Nilsequences".**

2.5 Quadrature Units Of Rotation

A discrete example is given to show that a local complete intersection applies a unit determinant and an invertible(identity) matrix to induce isomorphism. It is shown that the degree of a modular curve is equivalent to the representation modular form bounded by a constant, and multiplied by the LOGARITHM of an identity matrix i.e, a conductor. This construction implies Fermats' Conjecture, and moreover, is a finite set. That is to say, an asymptotic Fermats' set. It is further demonstrated by showing that the Riemann hypothesis over finite fields gets an EXPONENTIAL ESTIMATE. Clearly, a logarithmation operation implies an inverse INVOLUTION, and thus any LOGRITHM will be the EXPONENT of an INVOLUTION. The identities too, therefore imply no further extension to the system of numbers, and so we expect that a -ve exponent must appropriately yield a +ve fraction i.e, a quadrature unit of rotation. Taniyama's Conjecture is then related to Fermat's Conjecture, and any other others of the same type for that matter. . . Finally, we can apply Sylows' Theorems to Fermats' Last Theorem:

Theorem 2.1

A finite group G whose order $||G||$ is divisible by a prime power p^k has subgroups of order p^k. ♡

This is sufficient proof of Fermats' Conjecture, and was the main objective for the translation of Ludvig Sylows' **"Theorems Sur Le Groupes De Substitutions".**

2.6 General Concerns Regarding Problems Of The Proof

Indeed it is very important to accept that there is no general accepted derivation of the **Born Rule.**[4] Robert Langlands has clearly pointed out the gaps yet to be clarified in the fusion of Number Theory, Representation Theory, and Algebraic Geometry. Formal classification fields that need to addressed are

- *The Trace Formula*, including:
  - **functoriality**;
  - **spectral gaps on non-archimedean fields**.
- *Geometric Theory*: This is rigorously addressed by Frederic Schullers' Lectures and subsequent books on **"The Geometric Anatomy Of Theoretical Physics"**. I think Algebraic closure over the finite fields of the complex conjugate is well defined.
- *Mirror Symmetry*: Holographic Duality.
- *Reciprocity*: Proof of Gauss' Quadratic Reciprocity Theorem
  `https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs`
- *Advanced Theory On Automorphic L-functions*: Proof of the existence of Class Fields.
  `http://publications.ias.edu/rpl/section/27`

2.7 Conclusion

Remark It is understood that state(basis) vectors satisfy the wave function(equation) since it is constructed by Hamiltonian Mechanics. In the paper by Yang-Mills on **"Conservation Of Isotopic Spin and Isotopic Gauge Invariance"**, its pointed out that charged particles with mass less than Pions and Protons should live

[4] "Refer to the paper **The Born Rule And Its Interpretation: By N.P. Landsman"**

long enough to be seen at high energy levels. Otherwise if their mass is greater, they have a short lifetime of 10^{-20} seconds to decay into Pions and Protons, and would so far escape detection. They note that in electrodynamics, the conservation of charge is a consequence of the equation of motion of the electron field alone, quite independently of the electromagnetic field. The question of the mass of the b quantum in the b field is beset with divergences, and thus dimensional arguments(i.e,VANISHING MASS) are not satisfactory. This is because the b field carries an isotopic spin and destroys such general conservation laws. This is indeed a case of quantization of particles that DO NOT EXIST. Is this Mathematically interesting and if anything True? According to Robert Langlands, verifying and proving a reductive Algebraic group over $\mathbb{C}$-groups does not mean the existence of automorphic Galois group. You must try and comprehend what this statement means in relation to the above. So, computing rational points on curves of genus 2, and implying its Fermats' Conjecture, is a representation theorem forcing modularity of the base change to be equivalent. This is not very precise and rich, but, a solid basis for understanding modular space, functions, and Hecke Operators

Chapter 3 Theorems On The Groups Of Substitutions

Introduction

- *By M.L. SYLOW in FREDRIKSTAD, NORWAY*
- *The Notation and Terms used by Mr.C Jordan*
- *Group Order*
- *Transformation Of Substitutions and Abelian Equations*
- *Transitive (regular)Groups*
- *Radical Soluble Equations*

It is known that if the order of a group substitutions is divisible by the prime number N, the group still contains a substitution of order n. This important theorem is held in another more general way as follow: "If the order of a group is divisible by n^α, n being prime, the group contains a partial bundle of order n^α." The same demonstrations of the theorem provides some other general properties of substitution groups. I will add a few more less general proposals which are related to it, or which follow from it, some of which, however, are already known by a work by Mr. E. Mathieu.
The notations and terms used are those of Mr. C. Jordan.

3.1 Theorems On The Groups Of Substitutions: 584

1. If G is a group of substitutions whose order N is divisible by the prime number n, we know that G contains a substitution of order n, but we can suppose more generally that it contains a group g of order n^α of which thereof each substitution is of an order divisor of n^α. We will denote the substitutions of g by $1\ \theta_1\ \theta_2 \ldots$ while the substitutions of G will be denoted by $1\ \psi_1\ \psi_2 \ldots$ Finally, we will suppose that G does not contain any partial group whose order is of power greater than n^α. Now G always contains permutable substitutions to g, namely the substitutions of the latter itself, but it is possible that it contains a greater number of them; In any case these substitutions form a group γ, which contains g, and whose order will be denoted by $n^\alpha\nu$; This number is in turn a divisor of N; So we can do;

$$N = n^\alpha \nu \hbar \tag{3.1}$$

The substitutions of the group γ will be denoted by $1\ \varphi_1\ \varphi_2 \ldots$ The θ are thus included among the φ, as well as those among the ψ.

3.2 Theorems On The Groups Of Substitutions: 585

Having said that, let us first demonstrate that the number ν must be prime to n. Let $x_\circ\ x_1\ x_2 \ldots$ be the letters that group G permute between them, and let $y_\circ$ a rational function of x, invariant by the substitutions of g but variable by any other substitutions. This function takes by substitutions of γ the ν different values of $y_\circ\ y_1\ y_2 \ldots\ y_{\nu-1}$. Each of these functions is invariable by substitutions of g but variable by any other substitutions. In fact, if y_1 is deduced from $y_\circ$ by the substitution φ_1, y_1 is invariant by the group transformed from g by φ_1, but variable for any other substitution; But φ_1 being permutable to g, the transformed group is merged with g. However, if one operates in the y 's the substitutions of γ, one will have between these quantities a group γ' thereafter transitive and isomorphic to γ. To have the order of it, it is necessary to divide that of γ by the number of substitutions φ which do not alter any of the $y's$, that is, by n^α. So the order of γ' is ν. If now

ν was divisible by n, γ' would have to contain a substitution of order n; a corresponding substitution φ_1 of γ should fulfill the condition

$$\varphi_1^n = \theta_\alpha \tag{3.2}$$

But since φ_1 is permutable to g, we see that in this case the substitutions $\theta_q\ \varphi_1^p$ would form a group of order $n^{\alpha+1}$ contained in G. This being contrary to the hypothesis, we concluded that ν is prime to n. It should be noted here that θ are the only substitutions of γ whose orders are of the powers of n. In fact, if φ_1 is a foreign substitution of γ to g, the substitutions $\theta_q\ \varphi_1^p$ form a group whose order is equal to $n^\alpha m$, m denoting the exponent of the lowest power of φ_1 that belongs to g. Now it is easy to see that the only powers of φ_1 which belong to g are those whose exponents are of multiples of m, hence it follows immediately that m is a divisor of the order φ_1. So if the order of φ_1 were a power of n, one would have

$$m = n^\beta \tag{3.3}$$

which is impossible, the group $\theta_q\ \varphi_1^p$ cannot be of order $n^{\alpha+\beta}$. The number $\hbar$ is not divisible by n either. To do this, let us imagine a rational function x invariable by the substitutions of γ, but variable by any other substitution. Let $\mathcal{Z}_\circ$ be this function, and let us represent it by $\mathcal{Z}_\circ\ \mathcal{Z}_1\ \mathcal{Z}_2 \ldots \mathcal{Z}_{\hbar-1}$, the $\hbar$ values it takes by the substitutions of G. Let us carry out in $\mathcal{Z}$ the substitutions of g ; By this, $\mathcal{Z}_\circ$ does not vary, but each of the other $\mathcal{Z}$ takes a number of the values that is a divisor of the order g, that is to say, a power of n. This power can be reduced to the unit; If for example $\mathcal{Z}_1$ was invariable by g

3.3 Theorems On The Groups Of Substitutions: 586

and that $\mathcal{Z}_1$ is deduced from $\mathcal{Z}_\circ$ by the substitution ψ_1, $\mathcal{Z}_\circ$ should be invariable by the group transformed from g by ψ_1^{-1}; Yet, the only group of order n^α contained in γ being g, ψ_1^{-1} should be permutable to g, which does not happen. If so we divide the functions $\mathcal{Z}_1 \ldots \mathcal{Z}_{\hbar-1}$ into systems, by bringing together those that are permutable to each other by the substitutions of g, the number of functions contained in each system will be a power of n. Therefore the number of $\hbar$ is of the form $np+1$. The order of g is therefore equal to the largest power of n that divides the order of G. The results obtained are thus summarized as follows:

Theorem 3.1

I. If n^α denotes the largest power of the prime number n which divides the order of the group G, this group contains another g of the order n^α; If moreover, $n^a\nu$ denotes the order of the largest group contained in G whose substitutions are permutable to g, the order of G will be of the form $n^\alpha\nu(np+1)$. ♡

2. Obviously g is not the only group of order n^α contained in G, except only in the case $p = 0$. But one could ask if G contains others than g and its transforms by the substitutions of G. That is what we are going to look for. Let g' be a group of order n^α contained in G but different from g, and let $1\ \theta_1'\ \theta_2' \ldots$ be its substitutions. Let us perform these substitutions in the $\mathcal{Z}$ functions, and let us assemble in systems those that exchange between them. As we have already said, the number of functions contained in each system must be a divisor of n^α; So we must have an equality of the form

$$np + 1 = n^\alpha + n^b + n^c + \ldots \tag{3.4}$$

$n^\alpha, n^b, n^c \ldots$ denoting the number of functions contained in the various systems. But this requires that at least one of the exponents $a\ b\ c \ldots$ to be null.; In other words, at least one of the functions $\mathcal{Z}$ must be invariant to all other substitutions of g'. Let $\mathcal{Z}_k$ be this function, and suppose that it is deduced from $\mathcal{Z}_\circ$ by the substitution

ψ_k. $\mathcal{Z}_k$ is only invariant by the substitutions $\psi_k^{-1}\varphi_\alpha\psi_k$; Moreover $\psi_k^{-1}\varphi_\alpha\psi_k$ is similar to φ_α, and among the φ_α there are θ whose orders are the powers of n. We now have

$$\theta_b{}' = \psi_k^{-1}\,\theta_\alpha\,\psi_k \tag{3.5}$$

for all the values of b. So the group g' is therefore the transformation of g by ψ_k. If by the way we replace ψ_k with $\varphi_r\psi_k$, we obviously have the same transformed group. On the other hand ψ_k can only be replaced by $\varphi_r\psi_k$. Indeed, if one has

$$\psi_\ell^{-1}\theta_\alpha\psi_\ell = \psi_k^{-1}\theta_b\psi_k \tag{3.6}$$

3.4 Theorems On The Groups Of Substitutions: 587

for any values of a, it follows

$$\psi_k\psi_\ell^{-1}\theta_\alpha\psi_\ell\psi_k^{-1} = \theta_b \tag{3.7}$$

where we conclude

$$\psi_\ell\psi_k^{-1} = \varphi_r \tag{3.8}$$

or

$$\psi_\ell = \varphi_r\psi_k \tag{3.9}$$

We can thus state this theorem:

Theorem 3.2

Everything being posed as in the previous theorem, the group G contains precisely $np+1$ distinct groups of order n^α; They are all obtained by transforming any one of them by the substitutions of G, all being given by $n^\alpha\nu$ distinct transformants.

♡

By a similar reasoning we see that any group contained in G of order n^β, β being less than α, is the transform of a group contained in g by a substitution of G, and that there are at least $n^\alpha\nu$ ways of obtaining it by transformation. It is indeed possible that there are more, since the relation

$$\psi_k\psi_\ell^{-1}\theta_\alpha\psi_\ell\psi_k^{-1} = \theta_b \tag{3.10}$$

we cannot conclude

$$\psi_\ell\psi_k^{-1} = \varphi_r \tag{3.11}$$

unless it takes place for any value of α.

3. We will now deal with the group G. Let us form the transformations of substitutions $1\ \theta_1\ \theta_2\ldots$ by one of them; By this we only reproduce them in another order, we have a substitution between the substitutions θ themselves. If we transform them successively by all the substitutions of g, one has a group of substitutions; This is indeed the result of the identity:

$$\theta_b^{-1}\theta_a^{-1}\theta_r\theta_a\theta_b = (\theta_a\theta_b)^{-1}\theta_r(\theta_a\theta_b) \tag{3.12}$$

The group between the θ that we obtain is necessarily intransitive, the identical substitution at least being invariant by the transformations; but there are also other invariant substitutions, as we shall see. In fact, we can assemble into systems substitutions that are exchanged between themselves by the transformations; Once this is done, the transformations will produce a transitive group between the divisor of the order of the corresponding group; But one sees by a familiar reasoning that the order of this group is equal to n^α divided by the number of transformations that do not vary any of the substitutions of the system considered. Thus the number of

substitutions contained in each system is a power of n. The identical substitution being invariant, one must have an equality of the form

$$n^\alpha = 1 + n_1^\alpha + n^b + \dots \tag{3.13}$$

3.5 Theorems On The Groups Of Substitutions: 588

where $1\ n^\alpha\ n^b \dots$ are the number of the substitutions of the various systems. This requires that at least $n-1$ of the exponents $a\ b$ to be null. There is therefore in the group g at least n substitutions, including the identical substitution y, which are invariant; In other words there are in g at least n exchangeable substitutions with all the substitutions of the group. Now since, two substitutions are exchangeable, so are their powers also, there will always be among the substitutions exchangeable to all others a substitution of order n. Let $\theta_\circ$ be this substitution, and $y_\circ$ be a rational function in x, invariant by $\theta_\circ^\iota$ but variable by any other substitution, and represented by $y_\circ\ y_1\ y_2 \dots$ the $n^{\alpha-1}$ values it takes through the substitutions of g. By performing in the y the substitution of g one will have between these functions a group isomorphic to g whose order is obviously $n^{\alpha-1}$. By virtue of what has just been demonstrated, this group must contain a substitution of order n exchangeable for all substitutions of the group. Let θ_1 now be a corresponding substitution of g. Performed n times in a row θ_1 must reduce all the y 's to their primitive places, so

$$\theta_1^n = \theta_\circ^\alpha. \tag{3.14}$$

Moreover, if θ denotes any substitution of g, θ_1 must be the same substitution between the y 's as its transform by θ, that is to say, we have

$$\lambda^{-1}\theta_1\theta = \theta_1^b\theta_1. \tag{3.15}$$

The $\theta_\circ^\iota\theta_\ell^k$ substitutions obviously constitute a group of order n^2. If now one forms a rational function of x invariant by $\theta_\circ^\iota\theta_1^k$, but variable by any other substitution, and that we reason about this function, as we reasoned on $y_\circ$, we see that g must contain a substitution θ_2 that fulfills the condition

$$\begin{aligned} \theta_2^n &= \theta_\circ^c\theta_1^d \\ \vartheta^{-1}\theta_2\vartheta &= \theta_\circ^e\theta_1^t\theta_2 \end{aligned} \tag{3.16}$$

Continuing in this way we prove the following theorem:

Theorem 3.3

III. If the order of a group is n^α, n being prime, any substitution ϑ of the group can be expressed by the formula

$$\begin{aligned} \vartheta = \theta_\circ^\iota\theta_1^k\theta_2^\ell \dots \theta_{\alpha-1}^r \text{ or} \\ \theta_\circ^n &= 1 \\ \theta_1^n &= \theta_\circ^\alpha \\ \theta_2^n &= \theta_\circ^b\theta_1^c \\ \theta_3^n &= \theta_\circ^d\theta_1^e\theta_2^f \\ &\dots \end{aligned} \tag{3.17}$$

♡

3.6 Theorems On The Groups Of Substitutions: 589

and where we have

$$\begin{aligned}\vartheta^{-1}\theta_\circ\lambda &= \theta_\circ\\ \vartheta^{-1}\theta_1\lambda &= \theta_\circ^\beta\theta_1\\ \vartheta^{-1}\theta_2\lambda &= \theta_\circ^\gamma\theta_1^\delta\theta_2\\ \vartheta^{-1}\theta_3\lambda &= \theta_\circ^\varepsilon\theta_1^\zeta\theta_2^\eta\theta_3\end{aligned} \tag{3.18}$$

It is seen that the composition factors of the groups are all equal to n, we can therefore state as a corollary the following:

Proposition 3.1

If the order of the algebraic equation is a power of a prime number, the equation is solvable by radicals. ♠

Assume that the group g is transitive and that the number of letters is equal to n^β. In this case the substitutions we have named $\theta_\circ$ is regular, that is, it moves all the letters, and that all these cycles contain the same number of letters; Otherwise it would not be obviously exchangeable with all group substitutions. Moreover, the group will be imprimitive; Indeed the substitutions will replace the letters contained in the same cycle $\theta_\circ$ with the letters of the same cycle. So the equation will split it by solving an equation of degree $n^{\beta-1}$ in $n^{\beta-1}$ equations of degree n; The equations of degree n will therefore be Abelian. Thus:

Theorem 3.4

IV. If the degree of an irreducible equation is n^β, n being prime, and that the order of the group is also a power of n, any of its roots will be determined by a sequence of β Abelian equations of degree n ♡

For the case $n = 2$ this last proposition has been demonstrated by $Mr.\ J.$ Petersen ($Om\ de\ Ligninger$, $der\ kunne\ loses\ ved\ Kvadratrod\ etc.\ Kjobenhavn$ 1871). These results can even be generalized. In fact, if the order of the group of the equation is equal to $n^\alpha m$, m being less than n, we have, using Theorem I, $p = 0$, $m = \nu$. As a result all substitutions of the group permutable to the partial groups which we have denoted by g. The group is therefore reduced to g, if we adjoin the functions we have denoted by $y_\circ\ y_1 \ldots$, and which are the roots of an equation whose order and degree are equal to m. If therefore the auxiliary equation is solvable by radicals, so is the given equation. From this follows an immediate consequence:

Theorem 3.5

V. If the order of an algebraic equation is $n^\alpha\ n_1^{\alpha_1}\ n_2^{\alpha_2}\ n_3^{\alpha_3}\ldots$,
$n\ n_1\ n_2\ n_3\ \ldots$ *being prime, if moreover we have*

$$\begin{aligned}n &> n_1^{\alpha_1}\ n_2^{\alpha_2}\ n_3^{\alpha_3}\ldots\\ n_1 &> n_2^{\alpha_2}\ n_3^{\alpha_3}\ldots\\ n_2 &> n_3^{\alpha_3}\ldots\end{aligned} \tag{3.19}$$

♡

the equation is solvable by radicals.

3.7 Theorems On The Groups Of Substitutions: 590

4. From the above one can also derive a simple proof of the theorem of $M.E.Mathieu$:

Proof Any transitive group between n^α letters, n denoting a prime number, contains a regular substitution of order n. (see the paper of $M.Liouville1861$)

Let G be a transitive group of degree $n^\alpha m$, and let N be its order. Now N is divisible by n^α; So let

$$N = n^{\alpha+\beta} m N' \tag{3.20}$$

N' being assumed to be prime to n; Let G' be the group of order $n^\beta N'$ which contains the substitutions of G which does not move x. Now G contains a group g of order $n^{\alpha+\beta}$, and the substitutions of the latter which do not move $x_\circ$ form a group g', whose order we will denote by n^γ. Now g' is obviously contained in G', so we have

$$\gamma < \beta \tag{3.21}$$

But if we denote by r the number of places which are successively occupied by $x_\circ$, when we make all the substitutions of g, we have as we know,

$$r n^\gamma = n^{\alpha+\beta} \tag{3.22}$$

So

$$r \geq n^\alpha \tag{3.23}$$

The number r is necessarily a power of n; Moreover what has just been demonstrated for $x_\circ$ also occurs for each of the x's. So each letter takes by the group (g) a number of places which is power of n equal or greater than n^α. If we now assume $m = 1$, we see that g must be transitive. This being so, g must contain a regular substitution as we have already said. The theorem is thus proved.

There is another case where we can also prove the existence of regular substitutions. Suppose indeed

$$\alpha = 1 \tag{3.24}$$

with

$$m \ < \ n. \tag{3.25}$$

Since

$$n^2 > m\, n \tag{3.26}$$

we concluded that each letter takes by the substitutions of g precisely n different places. If therefore, m brings together in the same system the letters that are exchanged between them, we will have m systems of n letter each. Now let c be a cycle of a substitution of g, c will represent a circular substitution of the n letters of a same system. Now if another substitution of g causes the same letters to undergo a displacement, this displacement will be nothing other than a power of c, because otherwise one could derive from the two substitutions a third one which is not of order n. So let θ be a substitution of g, we have

3.8 Theorems On The Groups Of Substitutions: 591

$$\theta = c_1\, c_2 \ldots c_r \tag{3.27}$$

c_k denotes a circular substitution between the letters of the k^{th} system. If now

$$r \ < \ m, \tag{3.28}$$

the group g must contain a substitution θ_1 which permutes the letters of the $(r \ + \ 1)^{th}$ system, and from what

has just be said we have

$$\theta_1 = c_1^{\delta}\, c_2^{\varepsilon} \ldots c_r^{\zeta} c_r \ + \ 1\, c_r \ + \ 2 \ldots c_s, \tag{3.29}$$

the number $\delta\, \varepsilon \ldots \zeta$ may be zero. We derive,

$$\theta^p \theta_1 = c_1^p + \delta\, c_2^{p+\varepsilon} \ldots c_r^p + \zeta\, c_r + \ 1\, c_r \ + \ 2 \ldots c_s. \tag{3.30}$$

Now, since the number of systems is inferior to n, we can determine p so that none of the numbers $p \ + \ \delta$, $p \ + \ \varepsilon, \ldots \ p \ + \ \zeta$ is equal to zero. We thus obtain a substitution having $r \ + \ s$ cycles; Continuing in this way one will eventually find a regular substitution.

Theorem 3.6

VI. A transitive group between n m letters, n being prime, and $m < n$, contains a regular substitution of order n. ♡

By virtue of these two theorems any transitive group between less than 12 letters contains regular substitutions. But already for degree 12 there are transitive groups which are, devoid of them. Thus the substitutions of the groups derived from

$$\begin{aligned} \theta_0 &= (x_\circ\ x_1\ x_2)\ (x_3\ x_4\ x_5)\ (x_6\ x_7\ x_8) \\ \theta_1 &= (x_3\ x_4\ x_5)\ (x_6\ x_7\ x_8)\ (x_9\ x_{10}\ x_{11}) \\ \vartheta &= (x_\circ\ x_3\ x_6\ x_9\ x_1\ x_4\ (x_8\ x_{11})(x_2\ x_5\ x_7\ x_{10}) \end{aligned} \tag{3.31}$$

are similar to $\theta_\circ$, and the others to the powers of φ. Another example is the group derived from $\theta_\circ\ \theta_1$ and the following substitutions:

$$\begin{gathered} (x_0\ x_3\ x_1\ x_4)\ (x_2\ x_5)\ (x_6\ x_9\ x_7\ x_{11})\ (x_8\ x_{10}) \\ (x_0\ x_7\ x_1\ x_6)\ (x_2\ x_5)\ (x_3\ x_9\ x_4\ x_{11})\ (x_5\ x_{10}). \end{gathered}$$

These two are of the order 72, and characterize equations solvable by radicals.

5. Let us now consider transitive groups of degree prime. Let n be the degree, N the order of the group. Since N is divisible by n but not divisible by n^2, we have

$$N = n\ \nu\ (n\ p\ + 1). \tag{3.32}$$

Suppose that the letters are arranged in such an order that a circular substitution of the group is expressed by

$$\theta = |k,\ \ k\ +\ 1|; \tag{3.33}$$

then the permutable substitutions to the group derived from θ are of the form $|k,\ \ k\ +\ 1|$.

3.9 Theorems On The Groups Of Substitutions: 592

Now $n\ \nu$ is equal to the order of the latter group, so ν is equal to the number of substitutions in the given group that are of the form $|k,\ \ a\ k|$; ν is therefore a divisor of $n - 1$. So we have this theorem;

Theorem 3.7

VII. The order of a transitive group between a prime number of letters is of the form $n\ \nu(n\ p\ +\ 1)$, where n is the degree, $n\ p\ + 1$ the number of essentially different regular substitutions, that is, which are not powers of each other, and where ν is the number of substitutions of the form $|k,\ \ a\ k|$, any circular substitutions being noted by $|k,\ \ k\ +\ 1|$. ♡

These are partly known from the researches of $M.\ E.\ Mathieu$, who has shown that there are at least $\frac{N}{n\,\nu}$, such a number can be deduced from the $|k,\ \ k\ +\ b|$ by transforming them by the substitutions of the group. What must be added to the propositions of $M.\ Mathieu$ to have the above theorem is therefore that all circular substitutions can be deduced in the manner mentioned, a point on which $M.\ Mathieu$ t seems to have retained doubts. Let us remember there are two propositions also due to $M.\ Mathieu$:

Proposition 3.2

1. *If* $p\ >\ 0$, ν *cannot be equal to 1*
2. *If* $p\ >\ 0$, *and* n *is of the form* $4\hbar\ +\ 3$, ν *cannot be equal to 2.*

♠

Given the order of N of a transitive group between n letters, our theorem allows us to determine the number of circular substitutions and the number of substitutions permutable to the group derived from a circular substitution. Indeed ν, being less than n, is completely determined by the congruence

$$\frac{N}{n}\ \equiv\ \nu\quad \mod n; \tag{3.34}$$

And then we have

$$n\,p\ +1=\frac{N}{n\,\nu}. \tag{3.35}$$

Let us take for example the group of degree $\frac{q^r-1}{q-1}$, q being a prime number, which can be deduced from the linear group with r indices. If r is an odd prime, it can happen that $\frac{q^r-1}{q-1}$ is a prime number. So let us do

$$\begin{aligned} n&=\frac{q^r-1}{q-1}\\ N&=\frac{q^r-1}{q}(q^r-\ q)(q^r-\ q^2)\ldots(q^r-q^{r-1}) \end{aligned} \tag{3.36}$$

3.10 Theorems On The Groups Of Substitutions: 593

Now we can easily see that q is a primitive root of the congruence

$$\mathcal{Z}^r\equiv 1\quad \mod\ n; \tag{3.37}$$

Therefore we have

$$\mathcal{Z}^{r-1}+\mathcal{Z}^{r-2}\ldots\mathcal{Z}+1\equiv(\mathcal{Z}-q)(\mathcal{Z}-q^2)\ldots(\mathcal{Z}-q^{r-1}). \tag{3.38}$$

If we now make

$$\mathcal{Z}\equiv q^r\equiv 1 \tag{3.39}$$

we obtain

$$(q^r-\ q)(q^r-\ q^2)\ldots(q^r-q^{r-1})\equiv r \tag{3.40}$$

That is,

$$\frac{N}{n}\equiv r. \tag{3.41}$$

If we choose the indices so that a circular substitution is represented by $|k,\ \ k\ +\ 1|$, the group will contain r substitutions of the form $|k,\ \ a\,k|$ namely $|k,\ \ q^\iota k|$; the number essentially of different circular substitutions will be $\frac{q^r-q}{r}(q^r-\ q^2)\ldots(q^r-q^{r-1})$. The formula $N=n\,\nu\,(n\,p\ +1)$ considerably reduces the number of divisors of the product $2\ .\ 3\ldots n$ suitable to denote the order of a transitive group. For example, if we make $n\ =\ 7$, ν must be equal to 6 or 3, except for radical solvable equations. But if there is a group of order

$7(7\,p\,+\,1)6$, there is also a group of order $7(7\,p\,+\,1)3$ containing those substitutions of the first group that are equivalent to an even number of transformations. To have the values of $7\,p\,+\,1$ it is therefore sufficient to examine the case $n\,=\,3$; Therefore $7\,p\,+\,1$ must be a divisor of the number $2\,.\,5,\ 4\,.\,3$, and consequently equal to one of the number $1,\ 2^3,\ 5\,.\,3,\ 5\,.\,3\,.\,2^3$, the third of which must be rejected, since there is no group of order $5\,.\,3$ between 6 letters. For $n\,=\,11$ there will be only 15 cases to examine etc. Let us now examine the composition of the groups in question. Let G and $\mathcal{H}$ be two transitive groups, and let G be contained in $\mathcal{H}$ and permutable at its substitutions. Let $n(n\,p\,+1)\nu$ be the order of G, and let $\theta_\circ\theta_1\ldots\theta_{n\,p}$ be essentially different circular substitutions. G thus contains $n(n\,p\,+1)$ groups of order $n:\theta_\circ^r\theta_1^r,\ldots\theta_{n\,p^r}$. If we transform these groups by any circular substitution of $\mathcal{H}$, which will be denoted by θ', we must reproduce them in another order; We have to make a substitution between the $(n\,p\,+1)$ groups. But it is easy to easy that if a group θ_i^r is not invariant by the transformation, it must be part of cycle of n groups. So at least one of the groups is invariable by transformation. If we assume that it is $\theta_\circ^r$, this group is permutable to θ', from which we conclude

$$\theta'=\theta_\circ^b. \tag{3.42}$$

Indeed, if we choose the indices so that

3.11 Theorems On The Groups Of Substitutions: 594

$$\theta_\circ=|k,\ k\,+\,1|, \tag{3.43}$$

there are among the $n(n\,-\,1)$ substitutions $|k,\ \ k\,+\,b|$ are of order n. All circular substitutions of $\mathcal{H}$ are therefore part of G. Conversely, if G and $\mathcal{H}$ contain the same circular substitutions and $\mathcal{H}$ contains G, H is composed with G. Let $n(n\,p\,+1)\nu$ be the order of G, the order of $\mathcal{H}$ will be $n(n\,p\,+1)\nu\,\nu_1$, ν_1 being a divisor of $\frac{n\,-1}{\nu}$. Substitutions of the form $|k,\ \ a\,k|$ contained in $\mathcal{H}$ are the powers of only one of them; let us denote this φ. Those belonging to G will consequently be the powers of ϑ_1^ν. Now it is easy to see that $\mathcal{H}$ derives from the substitutions $\theta_\circ\theta_1\ldots\theta_{n\,p}\varphi$. Indeed the group derived from these substitutions is contained in $\mathcal{H}$; On the other hand its order cannot be less than $n(n\,p\,+1)\nu\,\nu_1$, since it has $n\,p\,+\,1$ circular substitutions and $\nu\,\nu_1$ substitutions $|k,\ \ a\,k|$. Similarly, G derives from the substitutions $\theta_\circ\theta_1\ldots\theta_{n\,p}\vartheta_1^\nu$. G is therefore permutable to the substitutions of $\mathcal{H}$, if it permutable to ϑ; Now this happens, because first the transformations of $\theta_\circ\theta_1\ldots\theta_{n\,p}$ by ϑ are circular substitutions belonging to $\mathcal{H}$ and therefore to G; Secondly ϑ^{ν_1} is exchangeable to ϑ. Thus we have proved the following theorem:

Theorem 3.8

VIII. For a transitive group of degree prime to be composed with a partial group, it is necessary and sufficient that the second group has all the circular substitutions of the prime. ♡

Let an equation be given whose group is $\mathcal{H}$. If we form a root function invariant to the substitutions of G, but variable by any other substitution, it will obviously be the root of an Abelian equation of degree ν_1. By adjoining this function we reduce the group of the equation to G. If therefore an irreducible equation of degree n is composed, it becomes simple by the addition of the root of an Abelian equation, whose degree is a divisor of $n\,-\,1$. Assuming $p\,=\,0$, we come back to a known property of radical soluble equation.

[1–19]

Bibliography

[1] Nicolas Billerey and Ricardo Menares. “On the modularity of reducible mod l Galois representations”. In: *arXiv preprint arXiv:1309.3717* (2013).

[2] Jan Hendrik Bruinier et al. *The 1-2-3 of modular forms: lectures at a summer school in Nordfjordeid, Norway*. Springer Science & Business Media, 2008.

[3] Fred Diamond and Kenneth A Ribet. “l-adic modular deformations and Wiles’s “Main Conjecture””. In: *Modular Forms and Fermat’s Last Theorem*. Springer, 1997, pp. 357–373.

[4] Gerhard Frey and Hans-Georg Rück. “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves”. In: *Mathematics of computation* 62.206 (1994), pp. 865–874.

[5] Ben Green, Terence Tao, and Tamar Ziegler. “An inverse theorem for the Gowers U4-norm”. In: *Glasgow Mathematical Journal* 53.1 (2011), pp. 1–50.

[6] Grigory Kondyrev and Artem Prikhodko. “CATEGORICAL PROOF OF HOLOMORPHIC ATIYAH–BOTT FORMULA”. In: *Journal of the Institute of Mathematics of Jussieu* 19.5 (2020), pp. 1739–1763.

[7] Robert P Langlands. *Euler products*. Vol. 1. Yale University Press New Haven, 1971.

[8] Robert P Langlands. *On the functional equations satisfied by Eisenstein series*. Vol. 544. Springer, 2006.

[9] Solomon Lefschetz. “Intersections and transformations of complexes and manifolds”. In: *Transactions of the American Mathematical Society* 28.1 (1926), pp. 1–49.

[10] Solomon Lefschetz. “On the existence of loci with given singularities”. In: *Transactions of the American Mathematical Society* 14.1 (1913), pp. 23–41.

[11] Solomon Lefschetz. “On the fixed point formula”. In: *Annals of Mathematics* (1937), pp. 819–822.

[12] Barry Mazur and Andrew Wiles. “On p-adic analytic families of Galois representations”. In: *Compositio Mathematica* 59.2 (1986), pp. 231–264.

[13] Vijay M Patankar and CS Rajan. “Distinguishing Galois representations by their normalized traces”. In: *Journal of Number Theory* 178 (2017), pp. 118–125.

[14] KA Ribet. “Division fields of abelian varieties with complex multiplication”. In: *Mém. Soc. Math. France (NS)* 2.75-94 (1980), p. 81.

[15] Simon Saunders. “Derivation of the Born rule from operational assumptions”. In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 460.2046 (2004), pp. 1771–1788.

[16] ML Sylow. “Théoremes sur les groupes de substitutions”. In: *Mathematische Annalen* 5.4 (1872), pp. 584–594.

[17] Richard Lawrence Taylor. “On congruences between modular forms”. PhD thesis. Princeton University, 1988.

[18] AFM Ter Elst and Derek W Robinson. “Elliptic operators on Lie groups”. In: *Acta Applicandae Mathematica* 44.1-2 (1996), pp. 133–150.

[19] X Wan et al. “Iwasawa Theory for Unitary Groups”. PhD thesis. Ph. D. thesis, Princeton University, 2012.

Appendix A Mathematical Tools

This appendix covers some of the Mathematics used in this book. Briefly discussed is the properties of summation operators and linear equations. Here you will find the special functions that are relevant to our current application. These require algebraic techniques. Calculus is also necessary to understand much of this book, for it is almost always used in advanced topics.

A.1 Probability Measure

A wave function $\{\Psi \in L^2(\mathbb{R})\}$ is regarded as an algebraic state ψ on the C^*-algebra $\{B(L^2\mathbb{R})\}$ of all bounded operators on the Hilbert Space $L^2(\mathbb{R})$. This C^* algebra contains commutative sub-algebra $C_o\mathbb{R}$ given by all multiplication operators on $L^2(\mathbb{R})$ defined by continuous functions of $x \in \mathbf{R}$ that vanish at infinity. Roughly speaking, this is the C^*-algebra generated by the position operator. The restriction $\psi|C_o(\mathbb{R})$ is given by

$$C_o\mathbb{R}(f) = \int_{\mathbb{R}} dx \mid \Psi(x) \mid^2 f(x). \tag{A.1}$$

Born Rule If a system is in a state $\Psi \in H$, then the probability $P(a \in B|\Psi)$ that a result in $B \subset \mathbb{R}$ is found when a is measured equals

$$P(a \in B|\Psi = P^a_\Psi(B). \tag{A.2}$$

For a discrete non-degenerate spectrum, a measurement of an observable a will produce one of its eigenvalues $\lambda_\imath$ as a result, then

$$P(a = \lambda_\imath|\Psi) = |(e_\imath, \Psi)|^2 \tag{A.3}$$

In other words, if

$$\Psi = \sum_\imath c_\imath e_\imath \text{ with } \sum_\imath |c_\imath|^2 = 1, \text{ then } P(a = \lambda_\imath|\Psi) = |c_\imath|^2 \tag{A.4}$$